EXHIBIT 5

Upon being informed of the impact on our Amazon Web Services (AWS) resources, MSU's primary concern was to discern the character of data impacted by the attacker's access to our data. In particular, the scientific research and other experimental activity using the AWS resources presented our Information Security Incident Response team with several challenges in determining if sensitive data was subject to unauthorized access. As a result, our team had to develop forensics processes to assess the impact and a method to provide answers under time constraints to meet compliance-driven reporting requirements.

This incident response effort was considered a very "heavy lift" where our analysts had to learn the AWS CloudTrail processes without previous experience in the domain. Our team of two analysts and a supervisor spent two weeks analyzing and assessing the affected data. This effort included days of reading AWS documentation, scripting data parsers by hand to get the JSON data from AWS into a human-readable format, and involving end users to determine data relevance. In addition, the team was not working their regularly assigned duties for approximately one month to meet reporting requirements.

MSU ultimately determined that was no sensitive data in the AWS resources and was able to address the root cause of vulnerability in AWS.

Regards,

Tom Siu
Chief Information Security Officer
MSU Information Security
Michigan State University